

CLAIMS

- 1
2 1. A method for detecting malicious applications in an electronic messaging
3 environment, comprising:
4 implementing a security software application in an electronic messaging system
5 with connection to a data network;
6 providing a local configuration of the security software application on a local
7 messaging terminal, wherein the local configuration includes a list of at least one known
8 malicious application;
9 detecting an electronic message received or to be sent by a local messaging
10 terminal;
11 determining whether the electronic message includes any attachment;
12 if an attachment is included with the electronic message, using the security
13 software application to check the attachment for any malicious application based on the
14 list of at least one known malicious application;
15 refreshing the local configuration of the security software application from a
16 globally replicated public folder within the electronic messaging system on a desired
17 periodic basis.
18
- 19 2. The method of claim 1, wherein implementing a security software application
20 on a local messaging terminal includes implementing an add-in software component to
21 an electronic message client software of the electronic messaging system.
22
- 23 3. The method of claim 2, wherein the electronic message client software resides
24 in a host server for the local messaging terminal.
25
- 26 4. The method of claim 1, wherein the security software application includes a
27 dynamic link library (DLL) application.

1

2 5. The method of claim 1, further comprising:
3 prompting an error message on the local messaging terminal when the attachment
4 to the electronic message matches a name on the list of the at least one known malicious
5 application.

6

7 6. The method of claim 5, further comprising:
8 blocking the matched attachment from being opened or sent.

9

10 7. The method of claim 1, wherein the list of at least one known malicious
11 application includes a list of known virus filenames.

12

13 8. The method of claim 1, wherein the local configuration of the security
14 software application includes:

15 an option to enable a checking of an attachment for any malicious application
16 based on the list of at least one known malicious application;

17 an option to add or remove a known malicious application from the list of at least
18 one known malicious application; and

19 an option to restrict an attachment type.

20

21 9. The method of claim 1, wherein the local configuration of the security
22 software application includes an option to set a time for the desired periodic basis to
23 refresh the local configuration.

24

25 10. A method for detecting malicious applications in an electronic messaging
26 environment, comprising:

1 implementing a security software application in an electronic messaging system
2 with connection to a data network;

3 providing a local configuration of the security software application on a local
4 messaging terminal, wherein the local configuration includes a list of at least one
5 application type;

6 detecting a receipt of an electronic message sent to a local messaging terminal;

7 determining whether the electronic message includes any attachment;

8 if an attachment is included with the electronic message, using the security
9 software application to check the attachment for any malicious application based on the
10 list of at least application type;

11 refreshing the local configuration of the security software application from a
12 globally replicated public folder within the electronic messaging system on a desired
13 periodic basis.

14

15 11. The method of claim 10, wherein implementing a security software
16 application on a local messaging terminal includes implementing an add-in software
17 component to an electronic message client software of the electronic messaging system.

18

19 12. The method of claim 11, wherein the electronic message client software
20 resides in a host server for the local messaging terminal.

21

22 13. The method of claim 10, wherein the local configuration of the security
23 software application includes:

24 an option to enable a checking of an attachment for any malicious application
25 based on a list of at least one known malicious application;

26 an option to enable a checking of an attachment for a restricted application type
27 based on the list of at least one application type; and

1 an option to add or remove an application type from the list of at least one
2 application type.

3
4 14. The method of claim 10, wherein the list of at least one application type
5 comprises executable application types.

6 15. The method of claim 14, wherein using the security software application to
7 check the attachment comprises:

8 determining whether the attachment is of one of the executable application types
9 listed in the list of at least one application type; and

10 if the attachment is of one of the executable application types, blocking the
11 attachment from being opened or sent through the electronic messaging system.

12
13 16. The method of claim 10, wherein the list of at least one application type
14 comprises application types not capable of containing malicious applications.

15
16 17. The method of claim 16, wherein using the security software application to
17 check the attachment comprises:

18 determining whether the attachment is of one of the application types not capable
19 of containing malicious applications; and

20 if the attachment is of one of the application types not capable of containing
21 malicious applications, allowing the attachment to be opened or sent through the
22 electronic messaging system.

23
24 18. The method of claim 10, wherein the local configuration of the security
25 software application includes an option to set a time for the desired periodic basis to
26 refresh the local configuration.

27